

ON THE NON-ARCHIMEDEAN METRIC MAHLER MEASURE

PAUL FILI AND CHARLES L. SAMUELS

ABSTRACT. Recently, Dubickas and Smyth constructed and examined the metric Mahler measure and the metric naïve height on the multiplicative group of algebraic numbers. We give a non-Archimedean version of the metric Mahler measure, denoted M_∞ , and prove that $M_\infty(\alpha) = 1$ if and only if α is a root of unity. We further show that M_∞ defines a projective height on $\overline{\mathbb{Q}}^\times / \text{Tor}(\overline{\mathbb{Q}}^\times)$ as a vector space over \mathbb{Q} . Finally, we demonstrate how to compute $M_\infty(\alpha)$ when α is a surd.

1. INTRODUCTION

Let K be a number field and v a place of K dividing the place p of \mathbb{Q} . Let K_v and \mathbb{Q}_p denote the respective completions. We write $\|\cdot\|_v$ to denote the unique absolute value on K_v extending the p -adic absolute value on \mathbb{Q}_p and define

$$|\alpha|_v = \|\alpha\|_v^{[K_v:\mathbb{Q}_p]/[K:\mathbb{Q}]}$$

for all $\alpha \in K$. Define the *Weil height* of $\alpha \in K$ by

$$H(\alpha) = \prod_v \max\{1, |\alpha|_v\}$$

where the product is taken over all places v of K . Given this normalization of our absolute values, the above definition does not depend on K , and therefore, H is a well-defined function on $\overline{\mathbb{Q}}$. Clearly $H(\alpha) \geq 1$, and by Kronecker's Theorem, we have equality precisely when α is zero or a root of unity.

We further define the *Mahler measure* of $\alpha \in \overline{\mathbb{Q}}$ by

$$M(\alpha) = H(\alpha)^{\deg \alpha}$$

where $\deg \alpha$ denotes the degree of α over \mathbb{Q} . It is simple to compute the Mahler measure of α in terms of its minimal polynomial f_α over \mathbb{Z} . If we write

$$f_\alpha(z) = A \cdot \prod_{n=1}^N (z - \alpha_n)$$

then, since H is invariant under Galois conjugation over \mathbb{Q} , we have that

$$(1.1) \quad M(\alpha) = \prod_{n=1}^N H(\alpha_n).$$

Certainly $M(\alpha) = 1$ if and only if α is a root of unity. As part of an algorithm for computing large primes, D.H. Lehmer [7] asked if there exists a sequence of

2000 *Mathematics Subject Classification.* Primary 11R04, 11R09.

Key words and phrases. Weil height, Mahler measure, Lehmer's problem.

algebraic numbers, none of which are roots of unity, whose Mahler measures tend to 1. The smallest Mahler measure that he found occurs when γ is a root of

$$\ell(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$$

in which case $M(\gamma) = 1.17\dots$. Since Lehmer's famous paper, many algorithms have been implemented to find numbers of small Mahler measure (see [8, 9, 10], for instance), and all have failed to produce an algebraic number of Mahler measure smaller than $M(\gamma)$. This led to the conjecture, now known as Lehmer's conjecture, that there does not exist such a sequence.

Conjecture. There exists a constant $c > 1$ such that $M(\alpha) \geq c$ whenever $\alpha \in \overline{\mathbb{Q}}^\times$ is not a root of unity.

Although many special cases have been established (see, for example, [2, 12, 13]), Lehmer's problem remains open in general. The best known universal lower bound on $M(\alpha)$ is due to Dobrowolski [3], who proved that

$$(1.2) \quad \log M(\alpha) \gg \left(\frac{\log \log \deg \alpha}{\log \deg \alpha} \right)^3$$

whenever α is not a root of unity.

Recently, Dubickas and Smyth [6] defined and studied the metric Mahler measure on the multiplicative group of algebraic numbers. Specifically, let

$$\mathcal{X}(\overline{\mathbb{Q}}^\times) = \{(\alpha_1, \alpha_2, \dots) : \alpha_n \in \overline{\mathbb{Q}}^\times, \alpha_n = 1 \text{ for a.e. } n\}.$$

That is, each element $(\alpha_1, \alpha_2, \dots) \in \mathcal{X}(\overline{\mathbb{Q}}^\times)$ must have $\alpha_n = 1$ for all but finitely many positive integers n . Also define the map $\tau : \mathcal{X}(\overline{\mathbb{Q}}^\times) \rightarrow \overline{\mathbb{Q}}^\times$ by $\tau(\alpha_1, \alpha_2, \dots) = \alpha_1 \alpha_2 \cdots$ and observe that τ is a group homomorphism. Define the *metric Mahler measure* by

$$(1.3) \quad M_1(\alpha) = \inf \left\{ \prod_{n=1}^{\infty} M(\alpha_n) : (\alpha_1, \alpha_2, \dots) \in \tau^{-1}(\alpha) \right\}$$

and note that $M_1(\alpha\beta) \leq M_1(\alpha)M_1(\beta)$ for all $\alpha, \beta \in \overline{\mathbb{Q}}^\times$. Using the triangle inequality for the Weil height, one verifies easily that

$$(1.4) \quad M(\alpha) \geq M_1(\alpha) \geq H(\alpha)$$

which implies, in particular, that $M_1(\alpha) = 1$ if and only if α is a root of unity. This means that the map $(\alpha, \beta) \mapsto \log M_1(\alpha\beta^{-1})$ defines a metric on the quotient group $\mathcal{G} = \overline{\mathbb{Q}}^\times / \text{Tor}(\overline{\mathbb{Q}}^\times)$. In addition, Dubickas and Smyth prove that $M_1(\alpha) = M(\alpha)$ whenever α is a rational number, a Pisot number, a Salem number, or a product of such numbers. Although it is too technical to include here, they further show how to compute $M_1(\alpha)$ when α is a surd.

In this paper, we examine the following non-Archimedean version of the metric Mahler measure. Define

$$(1.5) \quad M_\infty(\alpha) = \inf \left\{ \max_{n \geq 1} M(\alpha_n) : (\alpha_1, \alpha_2, \dots) \in \tau^{-1}(\alpha) \right\}$$

and note that $M_\infty(\alpha\beta) \leq \max\{M_\infty(\alpha), M_\infty(\beta)\}$ for all $\alpha, \beta \in \overline{\mathbb{Q}}^\times$. Our first goal is to show that $M_\infty(\alpha) = 1$ if and only if α is a root of unity. This fact is nearly trivial in the case of M_1 , as it follows easily from inequality (1.4). Although we

know that $M(\alpha) \geq M_\infty(\alpha)$, we cannot conclude that $M_\infty(\alpha) \geq H(\alpha)$ because H does not have the strong triangle inequality. In fact, this inequality is false in general because, for example, $H(4) = 4$ but $M_\infty(4) \leq 2$. However, we are able to establish a slightly weaker version.

Theorem 1.1. *If α is a non-zero algebraic number and not a root of unity then*

$$(1.6) \quad M_\infty(\alpha) \geq \inf\{H(\gamma) : \gamma \in \mathbb{Q}(\alpha) \text{ and } H(\gamma) > 1\}.$$

Dobrowolski's Theorem (1.2) implies immediately that the right hand side of (1.6) is strictly greater than 1. By Northcott's Theorem [11], the set $\{\gamma \in \mathbb{Q}(\alpha) : T > H(\gamma) > 1\}$ is finite for every positive real number T . This means that the infimum in (1.6) is, in fact, achieved. Either result is enough to obtain the following corollary.

Corollary 1.2. *$M_\infty(\alpha) = 1$ if and only if α is a root of unity.*

In view of Corollary 1.2, the map $(\alpha, \beta) \mapsto \log M_\infty(\alpha\beta^{-1})$ defines a metric on \mathcal{G} . Like the metric Mahler measure M_1 , M_∞ induces the discrete topology on \mathcal{G} if and only if Lehmer's conjecture is true.

It is important to note that Corollary 1.2 is trivial under the assumption of Lehmer's conjecture. Indeed, if $M_\infty(\alpha) = 1$ and α is not a root of unity, then whenever α is written as a product, some element of the product must not be a root of unity. Hence, we obtain a sequence of points α_n , none of which are roots of unity, with $M(\alpha_n)$ tending to 1 as $n \rightarrow \infty$. Of course, this would contradict the conclusion of Lehmer's conjecture.

We now give some additional basic properties about M_∞ . Let K be a number field and $\alpha \in K$. For a rational prime p , we say that α is a *p-adic unit* if for every place v dividing p , we have that $|\alpha|_v = 1$. Of course, this definition does not depend on K . Further, it is well-known that α is a *p-adic unit* if and only if p divides neither the first nor the last coefficient of the minimal polynomial of α over \mathbb{Z} .

Theorem 1.3. *If $\alpha \in \overline{\mathbb{Q}}^\times$ and $r \in \mathbb{Q}^\times$ then $M_\infty(\alpha^r) = M_\infty(\alpha)$. Moreover, if p is the largest prime such that α fails to be a *p-adic unit* then $M_\infty(\alpha) \geq p$.*

In general, there is ambiguity in writing α^r for $r \in \mathbb{Q}$ because there may be many r th powers of α . However, all such powers lie in the same coset of $\text{Tor}(\overline{\mathbb{Q}}^\times)$ in $\overline{\mathbb{Q}}^\times$. It is obvious that M_∞ is invariant under multiplication by a root of unity so these elements must all have the same value. Theorem 1.3 further implies that M_∞ defines a projective height on \mathcal{G} when it is viewed as a vector space, written multiplicatively, over \mathbb{Q} . This vector space is studied extensively in [1], in which it is noted that, among other things, the Weil height defines a norm with respect to the usual absolute value on \mathbb{Q} .

As an example of the second statement of Theorem 1.3, consider the algebraic number $\gamma = 1 + \sqrt{5}$. It is computed easily that γ has minimal polynomial $x^2 - 2x - 4 \in \mathbb{Z}[x]$ so that γ fails to be a 2-adic unit but is a *p-adic unit* for all primes $p > 2$. In this case, Theorem 1.3 yields the bound $M_\infty(\gamma) \geq 2$. As another basic example, if α is rational then $M_\infty(\alpha)$ is bounded below by the largest prime that divides its numerator or denominator. In fact, we may apply Theorem 1.3 to compute precisely the value of the strong metric Mahler measure at any surd.

Corollary 1.4. *If α is rational and d is a positive integer then $M_\infty(\alpha^{1/d})$ equals the largest prime dividing the numerator or denominator of α .*

It is worth noting that Corollary 1.4 identifies a large class of cases of equality in the second statement of Theorem 1.3. Indeed, the primes dividing the numerator and denominator of α are the same as the primes such that $\alpha^{1/d}$ fails to be a p -adic unit.

2. HEIGHTS ON ABELIAN GROUPS

The method used to construct (1.3) and (1.5) is applicable on any abelian group with a function satisfying only a few simple properties. Although we cannot hope to prove anything particularly deep in such a general setting, it is worth exploring the basic facts before we prove our main results.

Let G be an abelian group written multiplicatively. We say that $\rho : G \rightarrow [1, \infty)$ is a *height on G* if the conditions

- (i) $\rho(1) = 1$
- (ii) $\rho(\alpha) = \rho(\alpha^{-1})$

are satisfied. We define the *zero set of ρ* to be

$$Z(\rho) = \{\alpha \in G : \rho(\alpha) = 1\}.$$

We further say that ρ is a *metric height on G* if we have that

$$\rho(\alpha\beta) \leq \rho(\alpha)\rho(\beta)$$

for all $\alpha, \beta \in G$. If ρ satisfies the stronger condition that

$$\rho(\alpha\beta) \leq \max\{\rho(\alpha), \rho(\beta)\}$$

for all $\alpha, \beta \in G$ then we say that ρ is a *strong (or non-Archimedean) metric height on G* . If σ is another height on G then we write $\sigma \leq \rho$ if $\sigma(\alpha) \leq \rho(\alpha)$ for all $\alpha \in G$. This yields a partial ordering of the set of all heights on G .

As we noted in the introduction, Dubickas and Smyth [4, 5, 6] studied several heights and metric heights on the group of algebraic numbers $\overline{\mathbb{Q}}^\times$. More specifically, they defined and studied the metric heights associated to the Mahler measure, the naïve height, and the length. Our first proposition generalizes several facts noted by Dubickas and Smyth regarding metric heights. The proof is only trivially different from several remarks made in [5] and [6], however, we include it here for the purposes of completeness.

Proposition 2.1. *Suppose that ρ is a metric height on the abelian group G . Then*

- (i) *$Z(\rho)$ is a subgroup of G .*
- (ii) *$\rho(\alpha) = \rho(\zeta\alpha)$ for all $\alpha \in G$ and $\zeta \in Z(\rho)$. That is, ρ is well-defined on $G/Z(\rho)$.*
- (iii) *The map $(\alpha, \beta) \mapsto \log \rho(\alpha\beta^{-1})$ defines a metric on $G/Z(\rho)$.*

Proof. If $\rho(\alpha) = \rho(\beta) = 1$ then we know that $\rho(\alpha\beta) \leq \rho(\alpha)\rho(\beta) = 1$. By definition of height we conclude that $Z(\rho)$ is indeed a subgroup of G . If $\zeta \in Z(\rho)$ then we have that

$$\rho(\alpha) = \rho(\zeta^{-1}\zeta\alpha) \leq \rho(\zeta^{-1})\rho(\zeta\alpha) = \rho(\zeta\alpha) \leq \rho(\zeta)\rho(\alpha) = \rho(\alpha)$$

which establishes that $\rho(\alpha) = \rho(\zeta\alpha)$. The final statement of the proposition follows from the triangle inequality. \square

Of course, Proposition 2.1 justifies our use of the word metric in the definition of metric height: although ρ does not necessarily define a metric on G , it is indeed a well defined metric on the quotient $G/Z(\rho)$. Thus it is important to identify the subgroup $Z(\rho)$ if we hope to fully understand a metric height ρ .

If we are given a height ρ on G it is possible to construct both a natural metric height and a natural strong metric height from ρ . Let

$$\mathcal{X}(G) = \{(\alpha_1, \alpha_2, \dots) : \alpha_n \in G, \alpha_n = 1 \text{ for a.e. } n\}.$$

Further, define the map $\tau : \mathcal{X}(G) \rightarrow G$ by $\tau(\alpha_1, \alpha_2, \dots) = \alpha_1 \alpha_2 \cdots$ and note that τ is a surjective group homomorphism. As is done in [5] and [6] using the Mahler measure and naïve height, we define

$$(2.1) \quad \rho_1(\alpha) = \inf \left\{ \prod_{n=1}^{\infty} \rho(\alpha_n) : (\alpha_1, \alpha_2, \dots) \in \tau^{-1}(\alpha) \right\}$$

and note that the map $\rho \mapsto \rho_1$ preserves the partial ordering of heights on G . In other words, if ρ and σ are heights on G with $\sigma \leq \rho$ then $\sigma_1 \leq \rho_1$. Now we establish a modification of the results of [5] and [6].

Theorem 2.2. *If ρ is a height on G then the following hold.*

- (i) ρ_1 is a metric height on G with $\rho_1 \leq \rho$.
- (ii) If σ is a metric height with $\sigma \leq \rho$ then $\sigma \leq \rho_1$.
- (iii) $\rho = \rho_1$ if and only if ρ is metric height.
- (iv) $(\rho_1)_1 = \rho_1$.

Proof. It is obvious that $\rho_1(\alpha) \geq 1$ for all $\alpha \in G$ and that $\rho_1(1) = 1$. Since $\alpha \mapsto \alpha^{-1}$ is an automorphism of G and $\rho(\alpha) = \rho(\alpha^{-1})$ for all $\alpha \in G$, it is also clear that $\rho_1(\alpha) = \rho_1(\alpha^{-1})$. Since $\tau(\alpha, 1, 1, \dots) = \alpha$, we have that $\rho_1 \leq \rho$ as well. To prove the triangle inequality for ρ_1 we observe that

$$\begin{aligned} \rho_1(\alpha\beta) &= \inf \left\{ \prod_{n=1}^{\infty} \rho(\alpha_n) : (\alpha_1, \alpha_2, \dots) \in \tau^{-1}(\alpha\beta) \right\} \\ &\leq \inf \left\{ \prod_{n=1}^{\infty} \rho(\alpha_n) \prod_{m=1}^{\infty} \rho(\beta_m) : (\alpha_1, \alpha_2, \dots) \in \tau^{-1}(\alpha), (\beta_1, \beta_2, \dots) \in \tau^{-1}(\beta) \right\} \\ &= \rho_1(\alpha) \rho_1(\beta) \end{aligned}$$

which establishes (i).

To prove (ii), we observe that

$$\begin{aligned} \rho_1(\alpha) &= \inf \left\{ \prod_{n=1}^{\infty} \rho(\alpha_n) : (\alpha_1, \alpha_2, \dots) \in \tau^{-1}(\alpha) \right\} \\ &\geq \inf \left\{ \prod_{n=1}^{\infty} \sigma(\alpha_n) : (\alpha_1, \alpha_2, \dots) \in \tau^{-1}(\alpha) \right\} \\ &\geq \sigma(\alpha) \end{aligned}$$

where the last inequality follows from the triangle inequality for σ .

Obviously if $\rho = \rho_1$ then ρ is a metric height. To prove the converse, we assume that ρ is a metric height. Hence, statement (ii) implies that $\rho \leq \rho_1 \leq \rho$ which yields our result. The final statement follows immediately since ρ_1 is itself a height. \square

Indeed, Theorem 2.2 indicates that the definition (2.1) is a natural way of constructing a metric height out of an ordinary height. Not only do we obtain a metric height, but we obtain the largest metric height that is less than or equal to ρ . Furthermore, we need not attempt this construction with a height that is already known to be metric. For example, the Weil height H on $\overline{\mathbb{Q}}^\times$ is already a metric height so that applying (2.1) yields the Weil height again. The Mahler measure of an algebraic number α , however, does not have the triangle inequality, so this leads to the non-trivial construction studied in [6].

We now turn our attention to a non-Archimedean version of (2.1). Once again, we assume that ρ is a height on G and define

$$(2.2) \quad \rho_\infty(\alpha) = \inf \left\{ \max_{n \geq 1} \{\rho(\alpha_n)\} : (\alpha_1, \alpha_2, \dots) \in \tau^{-1}(\alpha) \right\}$$

so that the product in (2.1) is replaced with a maximum. As in the construction of ρ_1 , we observe that the strong metric construction preserves the partial ordering of heights on G . We further note an analogue of Theorem 2.2 for ρ_∞ .

Theorem 2.3. *If ρ is a height on G then the following hold.*

- (i) ρ_∞ is a strong metric height on G with $\rho_\infty \leq \rho_1$.
- (ii) If σ is a strong metric height with $\sigma \leq \rho$ then $\sigma \leq \rho_\infty$.
- (iii) $\rho = \rho_\infty$ if and only if ρ is a strong metric height.
- (iv) $\rho_\infty = (\rho_1)_\infty = (\rho_\infty)_1 = (\rho_\infty)_\infty$.

Proof. The proofs of statements (i), (ii) and (iii) are nearly identical to proofs of the analogous statements in Theorem 2.2 so we do not include them here. To verify (iv) we note that

$$\rho_\infty \leq \rho_1 \leq \rho.$$

Since these inequalities are preserved by taking the strong metric height of each component, we obtain

$$(\rho_\infty)_\infty \leq (\rho_1)_\infty \leq \rho_\infty.$$

But it is clear from the (iii) that $(\rho_\infty)_\infty = \rho_\infty$ so that

$$(\rho_\infty)_\infty = (\rho_1)_\infty = \rho_\infty.$$

Finally, we note that ρ_∞ is certainly a metric height so that $(\rho_\infty)_1 = \rho_\infty$ by Theorem 2.2 (iii). \square

Theorem 2.3 implies that ρ_∞ is indeed a metric height as well so that we may apply Proposition 2.1 to it. The metric induced by ρ_∞ on $G/Z(\rho_\infty)$ is non-Archimedean, so every open or closed ball centered at 1 is a subgroup of $G/Z(\rho_\infty)$. Furthermore, for any $r \geq 1$, we set

$$B_r = \{\alpha \in G : \rho_\infty(\alpha) < r\}$$

and let S_r be the subgroup of G generated by the set $\{\alpha \in G : \rho(\alpha) < r\}$. It is clear that

$$S_r = \{\tau(\alpha_1, \alpha_2, \dots) : (\alpha_1, \alpha_2, \dots) \in \mathcal{X}(G) \text{ and } \rho(\alpha_n) < r \text{ for all } n\}.$$

If $\alpha \in S_r$ then $\alpha = \prod_{n=1}^\infty \alpha_n$ where $\rho(\alpha_n) < r$ for all n . Hence,

$$\rho_\infty(\alpha) \leq \max_{n \geq 1} \{\rho(\alpha_n)\} < r$$

so that $\alpha \in B_r$. To establish the opposite containment, note that if $\alpha \in B_r$ then $\rho_\infty(\alpha) < r$. Therefore, by definition of ρ_∞ there exists $(\alpha_1, \alpha_2, \dots) \in \tau^{-1}(\alpha)$ such that $\max_{n \geq 1} \{\rho(\alpha_n)\} < r$. It follows that $\alpha \in S_r$ and we have shown that

$$(2.3) \quad B_r = S_r.$$

It is worth noting that there is no analog of (2.3) for closed balls unless the infimum in ρ_∞ is always achieved on the boundary of the ball. If $\rho_\infty(\alpha) = r$ then we may simply conclude that for every $\varepsilon > 0$ there exists $(\alpha_1, \alpha_2, \dots) \in \tau^{-1}(\alpha)$ such that $\max_{n \geq 1} \{\rho(\alpha_n)\} < r + \varepsilon$. However, one cannot conclude that $\max_{n \geq 1} \{\rho(\alpha_n)\} \leq r$.

As an example of (2.2), we note that the Weil height H does not already have the strong triangle inequality. Therefore, we may find it interesting to apply (2.2) to it. However, we quickly realize that if $\alpha \in \overline{\mathbb{Q}}^\times$ then we may write $\alpha = (\alpha^{1/n})^n$ so that $H_\infty(\alpha) \leq H(\alpha^{1/n}) = H(\alpha)^{1/n}$. But, $H(\alpha)^{1/n}$ tends to 1 as n tends to ∞ implying that H_∞ is trivial. Of course, Corollary 1.2 establishes that M_∞ is non-trivial.

3. PROOFS OF OUR MAIN RESULTS

Before we prove Theorem 1.1 we recall the relevant definitions and notation. Suppose that K/F is any finite Galois extension of fields and let $G = \text{Aut}(K/F)$. Recall that the *norm from K to F* is the map $\text{Norm}_{K/F} : K \rightarrow F$ defined by

$$\text{Norm}_{K/F}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha).$$

It is obvious that right hand side is invariant under Galois conjugation by an element of G so that $\text{Norm}_{K/F}(\alpha)$ does indeed belong to F . Of course, if $\alpha \in F$ then $\text{Norm}_{K/F}(\alpha) = \alpha^{[K:F]}$. Furthermore, $\text{Norm}_{K/F}(\alpha\beta) = \text{Norm}_{K/F}(\alpha)\text{Norm}_{K/F}(\beta)$ so that the norm is a homomorphism from K^\times to F^\times .

Proof of Theorem 1.1. Assume $\alpha \in \overline{\mathbb{Q}}^\times \setminus \text{Tor}(\overline{\mathbb{Q}}^\times)$ and let $\varepsilon > 0$. Further suppose that $(\alpha_1, \alpha_2, \dots) \in \mathcal{X}(\overline{\mathbb{Q}}^\times)$ is such that $\alpha = \alpha_1 \alpha_2 \cdots$ and

$$(3.1) \quad \max\{M(\alpha_1), M(\alpha_2), \dots\} \leq M_\infty(\alpha) + \varepsilon.$$

Let $F = \mathbb{Q}(\alpha)$ and assume that K is a Galois extension of F containing each element α_n . Since $\alpha_n = 1$ for almost every n , the Galois group $G = \text{Aut}(K/F)$ is finite.

First assume that $\text{Norm}_{K/F}(\alpha_n)$ is a root of unity for all n . Then we have that

$$\alpha^{[K:F]} = \text{Norm}_{K/F}(\alpha) = \prod_{n=1}^{\infty} \text{Norm}_{K/F}(\alpha_n)$$

since the norm is a multiplicative homomorphism. Therefore, α is a root of unity which is a contradiction.

Now we may assume that there exists $\beta \in \{\alpha_1, \alpha_2, \dots\}$ such that $\text{Norm}_{K/F}(\beta)$ is not a root of unity. For simplicity, we let $H = \text{Aut}(K/F(\beta))$ and let S be a complete set of coset representatives of H in G . Also, assume that β_1, \dots, β_M are the conjugates of β over F and let $\hat{\beta} = \beta_1 \cdots \beta_M$. We obtain that

$$\text{Norm}_{K/F}(\beta) = \prod_{\sigma \in G} \sigma(\beta) = \prod_{\sigma \in S} \sigma(\beta)^{|H|} = \hat{\beta}^{|H|}$$

so that $\hat{\beta}$ must not be a root of unity.

Using (1.1), we know that $M(\beta)$ is the product of the heights of the conjugates of β over \mathbb{Q} . So the product of the heights of its conjugates over F is potentially smaller. Then using the triangle inequality for the Weil height, we find that

$$M(\beta) \geq \prod_{m=1}^M H(\beta_m) \geq H(\hat{\beta})$$

and it follows that

$$(3.2) \quad M_\infty(\alpha) + \varepsilon \geq H(\hat{\beta}) \geq \inf\{\gamma \in \mathbb{Q}(\alpha) : H(\gamma) > 1\}.$$

Since the right hand side of (3.2) does not depend on ε , we may let ε tend to zero to obtain the desired result. \square

Proof of Corollary 1.2. If α is a root of unity, then we have $M_\infty(\alpha) \leq M(\alpha) = 1$ so that $M_\infty(\alpha) = 1$. If α is not a root of unity, then Theorem 1.1 gives

$$M_\infty(\alpha) \geq \inf\{\gamma \in \mathbb{Q}(\alpha) : H(\gamma) > 1\}.$$

However, Dobrowolski's Theorem implies that the right hand side is strictly greater than 1 which establishes the corollary. \square

The proof of Theorem 1.3 will require a technical lemma.

Lemma 3.1. *Let $\alpha \in \overline{\mathbb{Q}}^\times$ and define $d(\alpha) = \min\{\deg(\zeta\alpha) : \zeta \in \text{Tor}(\overline{\mathbb{Q}}^\times)\}$. We have that $d(\alpha) \leq rd(\alpha^r)$ for all positive integers r and*

$$M_\infty(\alpha) = \inf \left\{ \max_{n \geq 1} \left\{ H(\alpha_n)^{d(\alpha_n)} \right\} : (\alpha_1, \alpha_2, \dots) \in \tau^{-1}(\alpha) \right\}.$$

Proof. To prove the first statement, let $f(x)$ denote the minimal polynomial of α^r over \mathbb{Z} . Hence, the polynomial $f(x^r)$ vanishes at α and has degree $r \deg \alpha^r$. It follows that $\deg \alpha \leq r \deg \alpha^r$. But then

$$\begin{aligned} rd(\alpha^r) &= r \cdot \inf\{\deg(\zeta\alpha^r) : \zeta \in \text{Tor}(\overline{\mathbb{Q}}^\times)\} \\ &= \inf\{r \deg(\zeta^r \alpha^r) : \zeta \in \text{Tor}(\overline{\mathbb{Q}}^\times)\} \\ &\geq \inf\{\deg(\zeta\alpha) : \zeta \in \text{Tor}(\overline{\mathbb{Q}}^\times)\} = d(\alpha). \end{aligned}$$

To prove the second statement, we first observe that $\deg(\alpha) \geq d(\alpha)$ so that

$$(3.3) \quad M_\infty(\alpha) \geq \inf \left\{ \max_{n \geq 1} \left\{ H(\alpha_n)^{d(\alpha_n)} \right\} : (\alpha_1, \alpha_2, \dots) \in \tau^{-1}(\alpha) \right\}.$$

Now assume that $\tau(\alpha_1, \alpha_2, \dots) = \alpha$ so that $\alpha = \prod_{n=1}^\infty \alpha_n$. For each n we select ζ_n such that $\deg(\zeta_n \alpha_n) = d(\alpha_n)$. We have that

$$\alpha = \prod_{n=1}^\infty (\alpha_n \zeta_n) \zeta_n^{-1},$$

and therefore,

$$\begin{aligned} M_\infty(\alpha) &\leq \max_{n \geq 1} \left\{ \max \left\{ H(\alpha_n \zeta_n)^{\deg(\alpha_n \zeta_n)}, H(\zeta_n^{-1})^{\deg(\zeta_n^{-1})} \right\} \right\} \\ &= \max_{n \geq 1} \left\{ H(\alpha_n)^{d(\alpha_n)} \right\} \end{aligned}$$

The result follows by taking the infimum of both sides over all $(\alpha_1, \alpha_2, \dots) \in \tau^{-1}(\alpha)$. \square

Proof of Theorem 1.3. We first prove that $M_\infty(\alpha^r) = M_\infty(\alpha)$ for all positive integers r . The strong triangle inequality implies immediately that

$$M_\infty(\alpha^r) \leq M_\infty(\alpha)$$

so we must prove the opposite inequality. By Lemma 3.1 we have that

$$M_\infty(\alpha) = \inf \left\{ \max_{n \geq 1} \left\{ H(\alpha_n)^{d(\alpha_n)} \right\} : (\alpha_1, \alpha_2, \dots) \in \tau^{-1}(\alpha) \right\}.$$

Each term $H(\alpha)^{d(\alpha)}$ is well-defined on the quotient group $\mathcal{G} = \overline{\mathbb{Q}}^\times / \text{Tor}(\overline{\mathbb{Q}}^\times)$. Hence, we may instead take the infimum over all $(\alpha_1, \alpha_2, \dots) \in \mathcal{X}(\mathcal{G})$ with $\tau(\alpha_1, \alpha_2, \dots) = \alpha$ and we obtain the same value. Applying both statements of Lemma 3.1 we obtain that

$$\begin{aligned} M_\infty(\alpha) &= \inf \left\{ \max_{n \geq 1} \left\{ H(\alpha_n)^{d(\alpha_n)} \right\} : \alpha = \prod_{n=1}^{\infty} \alpha_n \right\} \\ &\leq \inf \left\{ \max_{n \geq 1} \left\{ H(\alpha_n)^{rd(\alpha_n^r)} \right\} : \alpha = \prod_{n=1}^{\infty} \alpha_n \right\} \\ &= \inf \left\{ \max_{n \geq 1} \left\{ H(\alpha_n^r)^{d(\alpha_n^r)} \right\} : \alpha = \prod_{n=1}^{\infty} \alpha_n \right\} \end{aligned}$$

for all $\alpha \in \mathcal{G}$ and all positive integers r .

Now define $g_r : \mathcal{G} \rightarrow \mathcal{G}$ by $g_r(\alpha) = \alpha^r$ and note that g_r is an automorphism of \mathcal{G} . We have shown that

$$(3.4) \quad M_\infty(\alpha) \leq \inf \left\{ \max_{n \geq 1} \left\{ H(g_r(\alpha_n))^{d(g_r(\alpha_n))} \right\} : \alpha = \prod_{n=1}^{\infty} \alpha_n \right\}.$$

Since g_r^{-1} is also an automorphism, we may take the infimum on the right hand side of (3.4) over all $(\alpha_1, \alpha_2, \dots) \in \mathcal{X}(\mathcal{G})$ such that $\alpha = \prod_{n=1}^{\infty} g_r^{-1}(\alpha_n)$. We conclude that

$$\begin{aligned} M_\infty(\alpha) &\leq \inf \left\{ \max_{n \geq 1} \left\{ H(g_r(g_r^{-1}(\alpha_n)))^{d(g_r(g_r^{-1}(\alpha_n)))} \right\} : \alpha = \prod_{n=1}^{\infty} g_r^{-1}(\alpha_n) \right\} \\ &= \inf \left\{ \max_{n \geq 1} \left\{ H(\alpha_n)^{d(\alpha_n)} \right\} : g_r(\alpha) = \prod_{n=1}^{\infty} \alpha_n \right\} \\ &= \inf \left\{ \max_{n \geq 1} \left\{ H(\alpha_n)^{d(\alpha_n)} \right\} : \alpha^r = \prod_{n=1}^{\infty} \alpha_n \right\} \\ &= M_\infty(\alpha^r) \end{aligned}$$

which completes the proof of the first statement when r is a positive integer. If $r < 0$ is an integer then

$$M_\infty(\alpha^r) = M_\infty((\alpha^{-1})^{-r}) = M_\infty(\alpha^{-1}) = M_\infty(\alpha).$$

If we have $r/s \in \mathbb{Q}$ then

$$M_\infty(\alpha^{r/s}) = M_\infty((\alpha^{r/s})^s) = M_\infty(\alpha^r) = M_\infty(\alpha).$$

To prove the second statement we note that if α fails to be a p -adic unit then $M(\alpha) \geq p$. To see this, let $K = \mathbb{Q}(\alpha)$ and let v be a place of K such that $|\alpha|_v \neq 1$.

Since $M(\alpha) = M(\alpha^{-1})$ we may assume without loss of generality that $|\alpha|_v > 1$. Further, write

$$O_v = \{z \in K_v : |z|_v \leq 1\} \quad \text{and} \quad M_v = \{z \in K_v : |z|_v < 1\}$$

for the ring of v -adic integers in K_v and its unique maximal ideal, respectively. Let π_v be a generator of M_v so that whenever $|z|_v > 1$ we have that $|z|_v \geq |\pi_v|_v^{-1}$. It is also well-known that

$$(3.5) \quad |\pi_v|_v^{-[K:\mathbb{Q}]} = p^{f_v}$$

where p^{f_v} is the cardinality of the residue field O_v/M_v . We now notice that

$$\begin{aligned} M(\alpha) &= \prod_w \max\{1, |\alpha|_w\}^{\deg \alpha} \\ &\geq |\alpha|_v^{\deg \alpha} \\ &\geq |\pi_v|_v^{-[K:\mathbb{Q}]} \\ &= p^{f_v} \geq p. \end{aligned}$$

Now let $\varepsilon > 0$ and assume that $(\alpha_1, \alpha_2, \dots) \in \mathcal{X}(\overline{\mathbb{Q}}^\times)$ is such that $\alpha = \alpha_1 \alpha_2 \dots$ and

$$M_\infty(\alpha) \geq \max\{M(\alpha_n) : n \geq 1\} - \varepsilon.$$

Further assume that p is the largest prime such that α is not a p -adic unit. By our earlier remarks there exists n such that α_n fails to be a p -adic unit, and thus $M(\alpha_n) \geq p$ and

$$M_\infty(\alpha) \geq \max\{M(\alpha_n) : n \geq 1\} - \varepsilon \geq p - \varepsilon.$$

The result follows by letting ε tend to zero. \square

Proof of Corollary 1.4. Since $\alpha \in \mathbb{Q}$ we may write

$$\alpha = \prod_{n=1}^N q_n^{r_n}$$

where q_n are rational primes and r_n are non-zero integers. Assume that p is the largest of the primes q_n . Then the strong triangle inequality for M_∞ and Theorem 1.3 imply that

$$M_\infty(\alpha) \leq \max_{1 \leq n \leq N} M_\infty(q_n^{r_n}) = \max_{1 \leq n \leq N} M_\infty(q_n) \leq \max_{1 \leq n \leq N} q_n = p.$$

By the second statement of Theorem 1.3 we also know that $M_\infty(\alpha) \geq p$ so that $M_\infty(\alpha) = p$. Then applying the first statement again we obtain that

$$M_\infty(\alpha^{1/d}) = M_\infty(\alpha) = p. \quad \square$$

REFERENCES

- [1] D. Allcock and J.D. Vaaler, *A Banach space determined by the Weil height*, Acta Arith. **136** (2009), 279–298.
- [2] R. Breusch, *On the distribution of the roots of a polynomial with integral coefficients*, Proc. Amer. Math. Soc. **2** (1951), 939–941.
- [3] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. **34** (1979), no. 4, 391–401.
- [4] A. Dubickas and C.J. Smyth, *Length of the Sum and Product of Algebraic Numbers*, Math. Notes **77** (6) (2005), 787–793, Trans. from Mat. Zametki **77** (6) (2005), 854–860.

- [5] A. Dubickas and C.J. Smyth, *On metric heights*, Periodica Mathematica Hungarica **46** (2) (2003), 135–155.
- [6] A. Dubickas and C.J. Smyth, *On the metric Mahler measure*, J. Number Theory **86** (2001), 368–387.
- [7] D.H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. **34** (1933), 461–479.
- [8] M.J. Mossinghoff, *Algorithms for the determination of polynomials with small Mahler measure*, Ph.D. Thesis, University of Texas at Austin, 1995.
- [9] M.J. Mossinghoff, website, *Lehmer's Problem*, <http://www.cecm.sfu.ca/~mjm/Lehmer>.
- [10] M.J. Mossinghoff, C.G. Pinner and J.D. Vaaler, *Perturbing polynomials with all their roots on the unit circle*, Math. Comp. **67** (1998), 1707–1726.
- [11] D.G. Northcott, *An inequality on the theory of arithmetic on algebraic varieties*, Proc. Cambridge Philos. Soc., **45** (1949), 502–509.
- [12] A. Schinzel, *On the product of the conjugates outside the unit circle of an algebraic number*, Acta Arith. **24** (1973), 385–399. Addendum, ibid. **26** (1975), no. 3, 329–331.
- [13] C.J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*, Bull. London Math. Soc. **3** (1971), 169–175.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TEXAS AT AUSTIN, 1 UNIVERSITY STATION
C1200 AUSTIN, TX 78712

E-mail address: pfili@math.utexas.edu

MAX-PLANCK-INSTITUT FÜR MATHEMATIK, VIVATSGASSE 7, 53111 BONN, GERMANY

E-mail address: csamuels@mpim-bonn.mpg.de